



INFORMATIONEN ZUR DATENVERARBEITUNG NACH ARTIKELN 13 und 14 DER DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Liebe Mitarbeiterinnen und Mitarbeiter,

der Schutz Ihrer personenbezogenen Daten ist uns wichtig. Nach Artikeln 13 und 14 der EU-Datenschutz-Grundverordnung (DSGVO) sind wir verpflichtet, Sie darüber zu informieren, zu welchem Zweck und auf welcher Rechtsgrundlage wir Daten erheben, speichern oder weiterleiten und welche Datenschutzrechte gemäß den Artikeln 15 bis 22 der DSGVO Sie wahrnehmen können.

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern im Folgenden die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Schutz Ihrer Daten

Beschäftigtendaten enthalten Privatgeheimnisse der betroffenen Mitarbeiter und unterliegen einer besonderen Vertraulichkeit nach den Bestimmungen des Datenschutzes. Alle Mitarbeiter der DRK-Blutspendedienst Medizinische Dienstleistungen gemeinnützige GmbH und der DRK-Blutspendedienste Baden-Württemberg – Hessen gGmbH sowie Nord-Ost gGmbH sind auf die Einhaltung der Datenschutzbestimmungen verpflichtet worden.

Zum Schutz Ihrer persönlichen Daten hält die DRK-Blutspendedienst Medizinische Dienstleistungen gemeinnützige GmbH und bei Ihrem Einsatz in einem der Blutspendedienste die DRK-Blutspendedienste Baden-Württemberg – Hessen gGmbH sowie Nord-Ost gGmbH die Auflagen der EU-Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) strikt ein. Ihre persönlichen Daten werden nur für die Zwecke der Begründung, der Durchführung und der Beendigung des Beschäftigungsverhältnisses genutzt.

Keinesfalls werden Ihre Daten für Werbezwecke Dritter (kommerzielle Werbung, dies schließt auch die Werbung für sonstige Aufgaben des Deutschen Roten Kreuzes ein) genutzt oder



weitergegeben. Zum Schutz der Anlagen der Informationstechnologie gegenüber einem unberechtigten Zugriff Dritter sind Schutzmaßnahmen nach dem geltenden Stand der Technik eingeführt, der den Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entspricht.

Die folgenden Abschnitte dienen dazu, Sie über die mit dem Arbeitsverhältnis verbundene Verarbeitung personenbezogener Daten aufzuklären.

1. Wer ist für die Datenverarbeitung verantwortlich und an wen kann ich mich wenden?

Die zentrale verantwortliche Stelle der Datenverarbeitung ist die

DRK-Blutspendedienst Medizinische Dienstleistungen gemeinnützige GmbH

Saarburger Ring 10-12

68229 Mannheim

Telefonnummer für Beschäftigte: 0621-124792-30

E-Mailadresse für Beschäftigte: info@drk-medizin.de

Die Datenverarbeitung der Beschäftigtendaten erfolgt in den Personalabteilungen, Saarburger Ring 10-12 68229 Mannheim.

Die Speicherung der Daten erfolgt im Auftrag der DRK-Blutspendedienst Medizinische Dienstleistungen gemeinnützige GmbH auf einem zentralen Server des DRK-Blutspendedienstes Baden-Württemberg – Hessen.

Ihr Kontakt zum Datenschutzbeauftragten:

Externe Datenschutzbeauftragte der genannten verantwortlichen Stellen ist bis zum 30. April 2025 Herr Dr. Hartmut Voelskow. Ab dem 1. Mai 2025 übernimmt Herr Lukas Biniossek, Firma SCO-CON:SULT GmbH, Hauptstraße 27 53604 Bad Honnef diese Funktion. E-Mail: datenschutzbeauftragter@drk-medizin.de. Antworten vom Datenschutzbeauftragten erhalten Sie über eine abweichende externe E-Mailadresse. Prüfen Sie deshalb bitte auch auf eventuell fälschlich in den Spam-Ordner verschobene E-Mails.

Für Anfragen zu Ihren Datenschutzrechten identifizieren Sie sich bitte mit Ihrem vollen Namen, Geburtsdatum und Postadresse.



Schutz Ihrer elektronischen Kommunikation:

Für eine Kontaktaufnahme per E-Mail beachten Sie bitte, dass bei einer E-Mail-Kommunikation über die externe Leitung, also von Ihrer privaten E-Mailadresse aus und immer beim Senden an den Datenschutzbeauftragten, die Sicherheit Ihrer Mitteilungen auf dem Übertragungsweg nicht gewährleistet werden kann. Der externe E-Mailverkehr erfolgt unverschlüsselt oder nur abschnittsweise transportverschlüsselt, also nicht durchgehend geschützt vom Sender bis zum Empfänger.

Verwenden Sie für die Kommunikation mit der Personalabteilung bzw. Dienstplankoordinatoren bitte die Ihnen bekannte interne E-Mailadresse mit der Endung: @drk-medizin.de. Wenn Sie aus wichtigen Gründen (z. B. im Krankheitsfall) vom privaten Anschluss aus wichtige Informationen senden müssen, dann bedenken Sie bitte, dass eine Übermittlung ohne Dateiverschlüsselung das Risiko birgt, dass Dritte Ihre Daten auf dem Übertragungsweg zur Kenntnis nehmen oder verfälschen können. Das Risiko dafür trägt jeweils der Absender einer E-Mail.

2. Wofür verarbeiten wir Ihre Daten (Zweck der Verarbeitung) und auf welcher Rechtsgrundlage?

Ihre persönlichen Daten werden nur für die Zwecke der Begründung eines Beschäftigungsverhältnisses im Rahmen des Einstellungsverfahrens und anschließend nach Abschluss des Arbeitsvertrages für den Zweck der Abwicklung des Beschäftigungsverhältnisses sowie damit verbundener rechtlicher Verpflichtungen genutzt.

Die Personaldaten umfassen folgende Angaben

Unterlagen, die bereits aus den Bewerberdaten übernommen wurden:

- Identifikation, Adresse, gegebenenfalls die Telefonnummer.
- Qualifikations- und Weiterbildungsdaten mit Kopien von Zeugnissen der schulischen und beruflichen Aus- und Weiterbildung.
- Angaben zur beruflichen Erfahrung und der wesentlichen Stationen des bisherigen beruflichen Werdeganges, soweit Sie diese bei Ihrer Bewerbung angegeben hatten.
- Alter, wenn es bereits im Bewerbungsverfahren erforderlich war oder freiwillig angegeben wurde.
- Gegebenenfalls Daten aus beruflichen Netzwerken wie Xing oder LinkedIn.
- Gegebenenfalls Angaben des bisherigen oder eines früheren Arbeitgebers, wenn Sie diesen bei der Bewerbung als Referenz angegeben hatten.



Nach der Einstellung kommen Daten hinzu, die für die Entgeltabrechnung und die Abgaben an das Finanzamt sowie die Sozialversicherung erforderlich sind:

- Geburtsdatum, Religionszugehörigkeit, Familienstand.
- Krankenversicherungsnummern und Bankverbindung.

Unter den Beschäftigtendaten können im Laufe eines Arbeitslebens weitere Datenarten verschiedener Kategorien zusammenkommen.

Innerhalb der Personalabteilung:

- Qualifikations- und Weiterbildungsdaten, die fortlaufend während des Beschäftigungsverhältnisses erfasst werden.
- Daten und Stationen des beruflichen Werdeganges im Unternehmen und Zwischen-Beurteilungen, Zielerfüllung.
- Daten der jeweiligen Eingruppierungen und Einstufungen und Gehaltshöhen, ggf. auch von Sonderzahlungen, Zulagen.
- Zeiterfassungsdaten, Summen der Arbeitszeiten, Abwesenheitsdaten sowohl von Urlaubszeiten als auch von Krankheitstagen.
- ggf. die Angabe einer Schwerbehinderung oder Gleichstellung und Grad der Behinderung.
- ggf. eine freiwillige Angabe zum Gesundheitszustand.
- Daten und Informationen über besondere Ereignisse wie zum Beispiel auch Abmahnungen.
- Pfändungen/ Abtretungen.
- Unterlagen zur betrieblichen Altersversorgung sowie Entgeltumwandlung.

Die Rechtsgrundlage für alle genannten Kategorien ergibt sich aus § 26 des Bundesdatenschutzgesetzes zur Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses und zum Teil in Verbindung mit dem Steuerrecht und Sozialgesetzbuch, da alle diese Daten für die ordnungsgemäße Abwicklung des Beschäftigungsverhältnisses, für die nach Steuerrecht erforderlichen Meldungen an die Finanzämter und für die Zahlungen an die Sozial- und Krankenversicherungen erforderlich sind.

Darüber hinaus wird Ihr Name zur Prüfung gegen Sanktionslisten verwendet. Dabei erfolgt regelmäßig ein Abgleich mit Sanktionslisten der EU und der USA. Nur im Falle eines Treffers werden zur Detailprüfung auch weitere Daten wie Adresse und Geburtsdatum verwendet. Der Abgleich mit EU-Listen beruht auf der gesetzlichen Forderung nach dem deutschen



Außenwirtschaftsgesetz. Der Abgleich mit US-Listen erfolgt im berechtigten Interesse des Unternehmens aufgrund der hohen Strafen und ggf. sonstigen Sanktionen, die sonst dem Unternehmen gegenüber verhängt werden könnten. Die Vorgehensweise ist in der internen Richtlinie „Sanktionslistenprüfung Beschäftigte“ beschrieben. Im Falle eines eindeutigen Treffers (Übereinstimmung mit einem Eintrag in einer Sanktionsliste) werden Sie umgehend darüber informiert. Die Durchführung erfolgt ausschließlich in der jeweiligen Personalabteilung der Konzerngesellschaft. Eine Weitergabe zu diesem Zweck findet nicht statt.

Die Herkunft der Daten ist bis auf folgende Ausnahmen grundsätzlich direkt von Ihnen. Einzelne Angaben zu Qualifikations- und Weiterbildungsdaten können ggf. auch aus beruflichen Netzwerken wie Xing oder LinkedIn übernommen sein, Angaben zu Stationen des beruflichen Werdeganges ggf. von einem früheren Arbeitgeber übermittelt worden sein, wenn Sie diesen im Bewerbungsverfahren als Referenz angegeben hatten.

Revisionsprüfungen:

Im Rahmen von Revisionsprüfungen können in Einzelfällen personenbezogene Daten an die Firma Tasco weitergegeben werden. Der Zweck sind die an die Tasco ausgelagerten Prüfungen der Internen Revision. Die Information der Mitarbeitenden erfolgt über die vorherigen Ankündigungen der Revisionsprüfungen. Die Rechtsgrundlage wird unten im Abschnitt „Datenübermittlungen im Rahmen von Revisionsprüfungen“ angegeben.

Außerhalb der Personalabteilung:

- Speicherung von E-Mails im E-Mail-Dokumentationssystem.
Zweck und Rechtsgrundlage: Einhaltung der Archivierungspflichten nach Abgabenordnung und Handelsgesetzbuch. Wichtiger Hinweis: Ihre Korrespondenz mit der Personalabteilung wird nicht in das Dokumentationssystem aufgenommen.
- Benutzerdaten und Berechtigungsdaten in der Verwaltung der Systeme zur Datenverarbeitung
Zweck und Rechtsgrundlage: Abwicklung des Beschäftigungsverhältnisses sowie Schutzvorschriften in Bezug auf die Datenverfügbarkeit nach dem Datenschutzrecht, AMG und TFG.
- Mitarbeiterbezogene Datensatzkennungen bei allen Tätigkeiten in GMP-konformen Systemen zur Datenverarbeitung
Zweck und Rechtsgrundlage: Gesetzliche Forderung nach dem AMG und TFG, die Datenverarbeitung GMP-konform zu gestalten. Nach diesen Regeln ist für die



Rückverfolgbarkeit der Bearbeitung die Speicherung erforderlich, wer einen Datensatz angelegt und wer ihn zuletzt geändert hat.

- Zutrittsdaten im Transponderchip-basierten Zutrittskontrollsystem
Zweck und Rechtsgrundlage: Einerseits die Abwicklung des Beschäftigungsverhältnisses, um die notwendigen Zutritte für die Erledigung der dienstlichen Aufgaben zu ermöglichen und andererseits die Schutzvorschriften in Bezug auf die Zutrittsbegrenzungen nach dem Datenschutzrecht, AMG und TFG.
- Arbeitszeitdaten im System, mit dem Ihre Arbeitszeit für Abrechnungszwecke erfasst wird.
- Installationsdaten in persönlich zugeordneten mobilen elektronischen Geräten (Mobile Device Management)
Zweck: Zur Sicherstellung, dass nur geprüfte sichere Anwendungen laufen und Gewährleistung einer sicheren Kommunikation.
Rechtsgrundlage: Abwicklung des Beschäftigungsverhältnisses: Soweit die Mitarbeiter mobile Endgeräte für ihre berufliche Tätigkeit vom DRK-BSD bekommen, ist die Kontrolle und Verwaltung der installierten Anwendungen gemäß Zweckbestimmung zur Sicherstellung der Einhaltung vertraglicher Pflichten erforderlich.
- Dateieigenschaften von Office-Dateien: Diese sind zwar auch zu beachten, stehen aber unter alleiniger Kontrolle der Mitarbeiter. Personenbezogene Daten werden in Dateieigenschaften von Office-Dateien automatisiert abgelegt.
Außer der Angabe „zuletzt gespeichert von“ können vor einer Weitergabe einer Datei die personenbezogenen Angaben der Dateieigenschaften von jedem Mitarbeiter selbst gelöscht werden.
Zweck: Vom Hersteller der Office-Programme wird damit eine Rückverfolgbarkeit beabsichtigt, wer der Ersteller ist, auf welcher Vorlage das Dokument basiert, in welcher Organisation es erstellt wurde und wer es zuletzt geändert hat. Eine Rechtsgrundlage für die Notwendigkeit der Speicherung wird seitens des Arbeitgebers nicht festgelegt. Es besteht daher keine Verpflichtung, diese Daten vor Weiterleitung von Dateien gespeichert zu lassen.
Bei übernommenen und anschließend selbst weiterbearbeiteten Dateien sollen in eigener Verantwortung der Mitarbeiter nicht mehr korrekte Vorgängerangaben aus den Dateieigenschaften entfernt werden.



3. Wer bekommt meine Daten? (Kategorien von Empfängern der personenbezogenen Daten)

Die genannten Daten innerhalb der Personalabteilung:

Daten zu Ihrer Person werden intern im Konzernverbund nur in dem Umfang an die Leiter der Blutspendetermine der einzelnen Institute des DRK-Blutspendedienstes Baden-Württemberg – Hessen gGmbH und des DRK-Blutspendedienstes Nord-Ost weitergeleitet, wie es für den jeweiligen Einsatz zu einem Blutspendetermin zwingend erforderlich ist.

Eine externe Datenübermittlung findet zum Zweck der Abwicklung der Lohn- und Gehaltszahlungen, sowie Verrechnung und Abführung der Lohnsteuer- Sozialversicherungsbeiträge statt. Auftragnehmer für diese Abwicklung ist die Firma P&I Personal & Informatik AG, Kreuzberger Ring 56, 65205 Wiesbaden. Mit der Firma P&I wurde ein Vertrag zur Auftragsdatenverarbeitung nach den gesetzlichen Vorgaben abgeschlossen und die Firma sowie deren Mitarbeiter auf die Einhaltung der Vertraulichkeit und Privatgeheimnisse der Mitarbeiterdaten und auf die Einhaltung der notwendigen Sicherheitsmaßnahmen nach dem geltenden Stand der Technik verpflichtet.

Kontakt Daten des Datenschutzbeauftragten der Firma P&I:

E-Mail: Datenschutzbeauftragter@pi-ag.com

Weitere externe Datenübermittlungen finden nur auf der Grundlage geltender Gesetze statt. Das sind in der Regel die Übermittlungen an Finanzämter, die Sozialversicherung und gesetzliche Krankenversicherungen. An diese werden im Rahmen der Abrechnungen, auch über den Auftragnehmer, die Firma P&I Daten, w übermittelt. Weitere Datenübermittlungen können bei gegebenem Anlass an die Berufsgenossenschaft erfolgen und in anonymisierter Form an statistische Landesämter.

Nur in Ausnahmefällen können Übermittlungen an Ermittlungs- und Strafverfolgungsbehörden erforderlich werden, wenn diese mit hinreichender Begründung auf der Basis der entsprechenden gesetzlichen Grundlagen Daten anfordern.

Datenübermittlungen im Rahmen von Revisionsprüfungen

Rechtsgrundlage der Übermittlungen ist der Vertrag von TASCO mit dem DRK Blutspendedienst einschließlich aller Konzerngesellschaften über die revisorische Betreuung. TASCO nimmt die ausgelagerten Revisionsaufgaben für den BSD und alle Tochtergesellschaften wahr. Rechtsgrundlage für die Einbeziehung personenbezogener Daten von Mitarbeitenden daher Art. 6 Abs. 1 lit. b DSGVO in Bezug auf den Arbeitsvertrag.



Die Auslagerung erfolgt im Rahmen einer Beauftragung, bei der die Verantwortung für die Datenverarbeitung bei der jeweiligen Gesellschaft des DRK Blutspendedienstes verbleibt.

Die Revision übernimmt klassischerweise Kontroll- und Überwachungstätigkeiten im Unternehmen. Rechtsgrundlage hierfür ist auch die Wahrung berechtigter Interessen des BSD nach Art. 6 Abs. 1 lit f DSGVO. Unterliegen nun Beschäftigtendaten einer Prüfung gilt als Rechtsgrundlage für die Kontroll- und Überwachungstätigkeit der Internen Revision Art. 6 Abs. 1 lit. f DSGVO i.V.m. § 26 BDSG.

Falls der Verdacht einer dolosen Handlung festgestellt wird, müssen personenbezogene Daten zur Sachverhaltsaufklärung genutzt und als Prüfungsergebnis personenbezogene Aussagen getroffen werden. Die Rechtsgrundlage bei internen Sachverhaltsaufklärungen bzw. internen Ermittlungen ergeben sich vor allem aus der DSGVO, dem BDSG (§ 26 Abs. 1 Satz 2) und der Rechtsprechung des Bundesarbeitsgerichts.

Aufbewahrungsfristen bei der Firma Tasco: Revisionsunterlagen (Arbeitspapiere etc.) werden gemäß dem Handbuch der Tasco für sechs Jahre archiviert und anschließend ordnungsgemäß vernichtet. Diese Regelung gilt für Papier und digitale Unterlagen.

Die genannten Daten außerhalb der Personalabteilung:

Diese werden ausschließlich in der jeweiligen Fachabteilung des DRK-Blutspendedienstes Baden-Württemberg – Hessen gGmbH gespeichert und verarbeitet. Genaue Angaben dazu finden Sie zu jedem einzelnen Verfahren im Datenschutz-Verzeichnis der Verarbeitungstätigkeiten. Dieses Verzeichnis steht den Mitarbeitern im Intranet zur Verfügung.

Letzterer Absatz zuvor in Bezug auf Übermittlungen an Ermittlungs- und Strafverfolgungsbehörden gilt in Ausnahmefällen auch für Bewegungsdaten des Zutrittskontrollsystems und im Falle eines Diebstahls eines mobilen Gerätes für Daten des Mobile Device Managementsystems.

Benutzerdaten, Berechtigungsdaten und mitarbeiterbezogene Datensatzkennungen können gegebenenfalls bei behördlichen Prüfungen der Arzneimittelüberwachung und bei Auditierungen vor Ort eingesehen werden.

Daten im Rahmen von Meldungen nach dem Hinweisgeberschutzgesetz (HinSchG):

Personenbezogene Daten, die im Rahmen einer Meldung gemäß HinSchG an die externe Meldestelle gegeben werden, müssen nach Prüfung, außer bei Ablehnung einer Meldung durch die externe Stelle, an den Arbeitgeber zur weiteren Bearbeitung übermittelt werden.

- Daten der meldenden Person:



- Meldungen können anonym erfolgen, sie können mit Angabe des Namens erfolgen, aber mit dem Wunsch, dass der Name dem Arbeitgeber nicht offenbart wird, oder auf freiwilliger Basis kann der Weiterleitung an den Arbeitgeber zugestimmt werden. Im letzteren Fall werden nur Personen des Arbeitgebers die Identität des Meldenden erfahren, die mit der Aufarbeitung des Falls betraut werden und für die es wichtig ist, die Identität zu erfahren, um mit der meldenden Person selbst ein Gespräch führen zu können. Die gemeldete Person erfährt nicht die Identität des Meldenden. Die beteiligten Personen werden sensibilisiert, auch darauf zu achten, auf welchen Informationen Rückschlüsse auf die meldende Person möglich sind.
- Daten der gemeldeten Person:
- Die Identität der gemeldeten Person muss dem Arbeitgeber preisgegeben werden, da eine berechtigte Meldung nur dann von der externen Meldestelle weitergegeben wird, wenn ein Gesetzesverstoß im Unternehmen gemeldet wird. Der Personenkreis, der die Identität erfährt, wird so klein wie möglich gehalten und auf das notwendige Minimum begrenzt, um den Fall bearbeiten bzw. ein Ermittlungsverfahren einleiten zu können. Eine Weiterleitung an Ermittlungsbehörden wird erfolgen, wenn klare Nachweise für einen Gesetzesverstoß vorliegen. Die gemeldete Person wird sobald wie möglich über die Meldung des Falls und den Vorwurf ihr gegenüber in Kenntnis gesetzt. Wenn durch diese Information das Ermittlungsverfahren beeinträchtigt werden könnte, erfolgt sie vorübergehend jedoch noch nicht, solange bis diese Beeinträchtigung nicht mehr zu befürchten ist.
- Es handelt sich bei Meldungen nach dem HinSchG niemals um einen Routinevorgang, sondern immer um Einzelfälle. Deshalb kann kein Standardablauf in allen Punkten festgelegt werden. Eine datenschutzgerechte Vorgehensweise im Einzelfall wird durch entsprechende Sensibilisierung der jeweils eingebundenen Personen erreicht.

4. Werden Daten in ein Drittland oder an eine internationale Organisation übermittelt?

Datenübermittlungen von Beschäftigtendaten in andere Staaten finden nicht statt.

5. Wie lange werden meine Daten gespeichert?

Die Beschäftigtendaten von Mitarbeitern werden über die Dauer des Beschäftigungsverhältnisses aufbewahrt. Bei bestimmten Sonderfällen wie Abmahnungen, bestehen kürzere Löschfristen, sofern der Zweck der Erhebung entfällt. Sollten Sie davon



betroffen sein, wenden sie sich bitte an Ihre zuständige Personalabteilung. Für bestimmte Daten ist anschließend im Rahmen bestimmter Gesetze noch eine weitere Archivierung erforderlich:

- Die steuerrelevanten Daten werden bis zum Ende des 10. Jahres nach Beendigung des Beschäftigungsverhältnisses aufbewahrt.
- Bei Daten zu eventuellen gesundheitlichen Belastungen am Arbeitsplatz, gelten längere Aufbewahrungsvorschriften nach den jeweiligen einzelnen relevanten Rechtsvorschriften.

Personalakten in Papierform werden, soweit sie nicht zum Nachweis für Steuer- und Sozialversicherungsbehörden bzw. der betrieblichen Altersversorgung benötigt werden, bis zu 5 Jahre nach Beendigung des Arbeitsverhältnisses, längstens bis zur Beendigung eventueller Rechtsstreitigkeiten aus Anlass der Beendigung des Arbeitsverhältnisses aufbewahrt und danach vernichtet.

Die Daten, die nicht zu den Personaldaten zählen (oben genannte Datenarten Außerhalb der Personalabteilung) werden nach den jeweils zugrundeliegenden Rechtsvorschriften aufbewahrt und die detaillierten Angaben dazu werden im Datenschutz-Verzeichnis der Verarbeitungstätigkeiten zu den einzelnen Verfahren dokumentiert. Dieses Verzeichnis steht den Mitarbeitern im Intranet zur Verfügung.

6. Welche Datenschutzrechte habe ich?

Alle Anfragen zu Ihren Datenschutzrechten richten Sie bitte an die Personalabteilung der im Kapitel 1 genannten verantwortlichen Stelle.

Sie haben jederzeit ein **Recht auf Auskunft** über die bei uns zu Ihrer Person gespeicherten personenbezogenen Daten und auf die weiteren in Art. 15 DS-GVO im Einzelnen aufgeführten Informationen über die Datenverarbeitung. Sie können auf Antrag eine Kopie der personenbezogenen Daten über Ihre Person bekommen, die aktuell Gegenstand der Verarbeitung sind.

Eine solche Auskunftsanfrage sollten Sie jedoch nicht häufiger als höchstens einmal pro Jahr stellen, da auch die DS-GVO die Erteilung einer kostenfreien Auskunft auf Anfrage nur einmal pro Jahr vorschreibt.

Archivierte Unterlagen, die nicht mehr in den aktiven Datensätzen oder Personalakten vorliegen, können für die Auskunftserteilung nicht berücksichtigt werden, sind allerdings auch dem normalen Zugriff der Personalabteilung entzogen.



Berücksichtigen Sie bitte, dass wir aufgrund der Datenschutzforderungen Ihnen Ihre personenbezogenen Daten nur nach eindeutiger Identifizierung und nur persönlich übergeben oder zusenden dürfen. Dafür geben Sie bitte mindestens **Ihren vollständigen Namen, ggf. Ihr Geburtsdatum, und ggf. Ihre Postadresse** an. Diese Informationen müssen wir zur Identitätsprüfung mit den zuvor vorgelegten Daten vergleichen.

Sie haben das Recht, von uns unverzüglich die **Berichtigung** Sie betreffender unrichtiger personenbezogener Daten und ggf. die **Vervollständigung** unvollständiger personenbezogener Daten zu verlangen (Art. 16 DS-GVO), z. B. wenn Ihre Namens-, Adressangaben oder Daten der absolvierten Aus- und Weiterbildung fehlerhaft sind.

Sie haben das Recht, von uns zu verlangen, dass Sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der in Art. 17 DS-GVO im einzelnen aufgeführten Gründe zutrifft, z. B. wenn die Daten für die verfolgten Zwecke nicht mehr benötigt werden (**Recht auf Löschung**) und die gesetzlichen Aufbewahrungs- und Archivvorschriften gemäß Kapitel 5. einer Löschung nicht oder nicht mehr entgegenstehen.

Sie können die Löschung von Teilen der gespeicherten Daten verlangen, wenn Sie der Ansicht sind, dass diese nicht mehr für die Abwicklung des Beschäftigungsverhältnisses erforderlich sind. Wenn der Arbeitgeber der Ansicht ist, dass diese Daten weiterhin gespeichert bleiben müssen, wird er Ihnen dann die Rechtsgrundlage erläutern, aufgrund derer er die Fortführung der Speicherung dieser Daten anstrebt. Das kann zum Beispiel ein berechtigtes Interesse des Arbeitgebers sein, wenn er darlegen kann, dass dadurch und durch den guten Schutz Ihrer Daten Ihre Persönlichkeitsrechte nicht beeinträchtigt werden. Für eine Einigung ist im Zweifelsfall der Betriebsrat in das Gespräch einzubeziehen.

Sie haben das Recht, von uns die **Einschränkung der Verarbeitung** zu verlangen, wenn eine der in Art. 18 DS-GVO aufgeführten Voraussetzungen gegeben ist, z. B. wenn Sie Widerspruch gegen die Verarbeitung eingelegt haben, für die Dauer der Prüfung ob dem Widerspruch stattgegeben werden kann.

Das Recht auf **Datenübertragbarkeit** gem. Art. 20 DS-GVO zu einem anderen Arbeitgeber kann Ihnen durch Übergabe der Identifikations-, Kontakt- sowie Aus- und Weiterbildungsdaten oder der Dateien mit diesen Informationen, die Sie uns übermittelt haben, gewährt werden.

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten **Widerspruch** einzulegen, soweit diese nicht aufgrund einer gesetzlichen Vorschrift erfolgt oder zur Durchführung des Beschäftigungsverhältnisses erforderlich ist. Wir verarbeiten die personenbezogenen Daten



dann nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihren Interessen, Rechten und Freiheiten überwiegen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 21 DS-GVO).

Sie haben das Recht, sich über eine fehlerhafte Verarbeitung Ihrer personenbezogenen Daten durch uns bei der Datenschutz-Aufsichtsbehörde zu beschweren (**Beschwerderecht**). Zuständig ist jeweils die Datenschutzaufsichtsbehörde des Bundeslandes des Unternehmenssitzes der datenverarbeitenden Gesellschaft.

Die Adressen der Aufsichtsbehörden der Bundesländer finden Sie unter:
<https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html>

Für die DRK-Blutspendedienst Medizinische Dienstleistungen gemeinnützige GmbH mit Sitz in Mannheim ist die Behörde in Baden-Württemberg zuständig.

7. Einwilligung und Widerrufsrecht

Sollte eine Datenerfassung oder Datenverwendung auf der Basis Ihrer Einwilligung erforderlich werden, zum Beispiel zur Veröffentlichung Ihres Bildes im Internet, dann ist diese Einwilligung grundsätzlich freiwillig. Für Bilder gilt Letzteres jedoch nicht, wenn die Veröffentlichung, zum Beispiel für Tätigkeiten im Außendienst, bereits im Arbeitsvertrag vereinbart wurde. Die Ablehnung einer freiwilligen Einwilligung hat für Sie keine Nachteile. Sie werden im Einzelfall vor Einholung der Einwilligung darüber aufgeklärt.

Wenn Sie zur Erfassung oder Verwendung bestimmter Daten oder von Bildern eine Einwilligung erteilt haben, dann gilt ein uneingeschränktes Widerrufsrecht. Dieses richtet sich gegen jede weitere Verwendung der Daten oder Bilder in einem neuen Vorgang. Unter der Voraussetzung, dass die Löschung keinen unangemessenen Aufwand verursacht, werden nach Eingang Ihres Widerrufs die betroffenen Daten oder Bilder auch in der bereits bestehenden Speicherung oder Anwendung gelöscht.

Die Neuauflage einer bereits bestehenden Druckschrift wäre zum Beispiel mit einem unangemessenen Mehraufwand verbunden. In diesem Fall kann sich der Widerruf nur gegen die erneute Verwendung für die nächste Auflage auswirken.

8. Besteht für mich eine Pflicht zur Bereitstellung von Daten?

Bereits im Bewerbungsverfahren war es erforderlich, uns alle die personenbezogenen Daten zur Verfügung zu stellen, die wir für die Begründung des Beschäftigungsverhältnisses benötigten. Diese wurden in die Personaldaten übernommen und deren Verfügbarkeit ist dort



weiterhin erforderlich. Bei der Einstellung als Mitarbeiter bei uns sind Sie vertraglich und gesetzlich verpflichtet weitere Daten anzugeben, die für die Abwicklung des Beschäftigungsverhältnisses sowie die steuerrechtlichen und sozialversicherungsrechtlichen Belange vorliegen müssen. Zusätzlich können für spezielle Tätigkeiten bestimmte Eignungsangaben erforderlich sein, bevor solche Tätigkeiten ausgeführt werden dürfen. Die Information dazu erhalten Sie dann im Einzelfall.

Während des Beschäftigungsverhältnisses besteht für Sie die vertragliche Verpflichtung, uns jede Änderung Ihrer Kontaktdaten, Namensangaben, Kontoverbindung und des Familienstandes mitzuteilen. Eine Nichtbereitstellung kann die Abwicklung des Beschäftigungsverhältnisses erheblich behindern und zu Fehlern in steuerlichen sowie sozialversicherungsrechtlichen Mitteilungen und Berechnungen führen.

Sie sind weiterhin verpflichtet, uns die Teilnahmebescheinigungen oder Zertifikate von Weiterbildungen vorzulegen, die für Ihre Tätigkeit bei uns von Relevanz sind. Eine Nichtvorlage kann Nachteile für Ihren weiteren beruflichen Werdegang haben.

9. Inwieweit werden meine Daten für die Profilbildung (Scoring) genutzt?

Automatisierte Entscheidungen gemäß Art. 22 DSGVO oder andere Profiling-Maßnahmen nach Art. 4 Nr. DSGVO finden nicht statt.

10. Herausgeber

Herausgeber ist die verantwortliche Stelle, die im Kapitel 1 angegeben ist.